Volume 5, Issue 44   Atari Online News, Etc.   October 31, 2003

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Kevin Savetz
Peter West

=~=~=~=

A-ONE #0544   10/31/03

~ HighWire Gets Updated! ~ People Are Talking!   ~ Wrap-Mouse News!

```
        ~ UK: Extradite Spammers ~ Microsoft After Google ~ PC Ten Commandments
        ~ New Version of Hatari! ~ Longhorn Is Unveiled!  ~ 8-bit Ethernet Cart!
        ~ Sober-A Worm Spreads!  ~ Printer Cart Clones!   ~ Raster Music Tracker!

                        -* Apple Unleashes New Panther! *-
                      -* Internet Access Tax Ban Nears Vote! *-
                    -* House Votes Soon on Senate Anti-Spam Bill! *-
```

                              =~=~=~=

->From the Editor's Keyboard   "Saying it like it is!"
  """""""""""""""""""""""""""

Well, here we are celebrating one of the more enjoyable holidays of the
year, even though it's one of those holidays that is of no real significance
other than to the kids and candy manufacturers: Halloween! And I get to
miss most of it because I've been relegated to my study getting this week's
issue of A-ONE out and making sure that the dogs are kept quiet while my
wife gets to see all of of the scary visitors! I'll get to take a view
glimpses out the window to check out the trick-or-treaters on occasion,
however.

I enjoy this time of the year. While I'm not a big fan of having to clean
up the tons of leaves and stuff from the yard, I do enjoy watching the
leaves turning colors. And then Thanksgiving nears. I can't believe it's
almost November already! But, we're not there yet. I had better get this
issue out the door before the last of the "good" candy goes out the door
also, before I get a piece or two!

Until next time...

                              =~=~=~=

                    HighWire 0.1.5 Is Released

The open source browser HighWire has had another update, and this time the
changes are rather significant:

Clearly the most exciting change is that HighWire finally is capable of
viewing JPG/PNG graphics, and that the program now is able to download
and display images via remote connections!

In addition to this, HighWire is also able to store image bitmaps in
RAM to speed up the handling of graphics. Eg. swapping between pages
stored in the cache can benefit enormously from this! If not specified,
HighWire will use 100kb. It is important to point out, that if you
visit graphic intensive pages HighWire may have to spend time flushing
the cache memory over and over again if the cache memory limit is set
too low.

(Please refer to highwire.cfg on details how to set this up)

 Other interesting changes includes improved dithering and added
 support for 32k screen modes as well as better support for TrueColour
 and GrayScale. There has also been an optimisation of the cache scheme
 that lead to reduced flickering upon image rendering. Finally, a
 correction in the calculation of cache size for disk cached objects
 was made, and a bug causing the program to enter an infinite loop
 (when writing to the cache failed for some reason) was fixed.

Upon request from several people testing previous HighWire releases, it
is now enough to just enter eg. "www.atari.org" instead of "http://www.
atari.org". Keyboard shortcut CTRL+N will now opens a new (empty)
browser window.

To download the new release and read more about the project, please
visit:

http://highwire.atari-users.net

We hope that this new release will be useful, and also want to
encourage everyone to keep submitting bug reports and feedback!

Thank you,

HighWire development project

                              Wrap-Mouse

What is the right mouse-button good for on an Atari?

Did you ever wonder what the right mouse-button is for on an
Atari? Very few programs use it. But it's possible to map it to
perform other functions - double-clicks, Control- or Alt-clicks
etc. Left-handers may find it more convenient to click the right
rather than left button for selecting items etc.

These are just some of the functions offered by Wrap-Mouse, which
now is available in an English version. This AUTO-folder program
plus CPX has been made freeware by the author and translated by
DDP Translations into English. It's available for download from:

http://ddp.atari.org

Programs that do use the right button (some graphics applications,
Calamus...) can be excluded from the button mapping by entering
their names in a list in the configuring CPX.

But why is the program called 'Wrap-Mouse'? Because it also
incorporates a very sophisticated mouse accelerator that is fully
programmable for speeding up mouse movements from various
thresholds (of speed and movement distance) and because when the

cursor is moved off any edge of the screen it reappears on the opposite side - again programmable.

The down side of this little marvel? It needs to be used with Atari's XCONTROL.ACC control panel, as a CPX configures all of Wrap-Mouse's functions and the program won't run without it. ZCONTROL can be substituted up to a point, though only with MagiC's 'tidy up' function as the opening dialog sticks on the screen and can't be removed otherwise. Unfortunately the program will definitely NOT work with the more sophisticated COPS.ACC control panel :-(

Full details are in the README that is part of the ZIP.

Regards, /Peter/
(Peter A. West, London)

                New Version of the ST Emulator Hatari

Version 0.45 of the Atari ST emulator Hatari has been released. This is just a minor release on the way to version 0.50, but it fixes some ugly bugs from the last public version 0.40.

The following things have been changed:
- New build system (with a "configure" shell script).
- A disc image destroying bug in the MSA compression function has been fixed.
- It is now possible to redirect the printer output into a file.
- Experimental MIDI output support.
- Added the possibility to save memory snap shots.
- Pending HBL and VBL interrupts are now correctly emulated.
- Some speed improvements.
- GEMDOS HD emulation now also works with EmuTOS.

http://hatari.sourceforge.net/

                Atari 8-bit Ethernet Cartridge

Atari 8-bit fans will soon be able to connect to the internet via an Atari 8-bit Ethernet Cartridge (http://jybolac.virtualave.net/atari/a8ether/) being developed by Chris Martin. Based on the work already done in the Commodore 64 community, this adapter will allow you to take advantage of telnet, e-mail, web browsing and a web server via the Contiki Operating System. (http://www.dunkels.com/adam/contiki/)

For more information, including pictures and schematics, please visit the Atari 8-bit Ethernet Cartridge development page.

http://jybolac.virtualave.net/atari/a8ether/

                Raster Music Tracker - RMT 1.14

New RMT tracker version 1.14 is out. See the file changes.txt to know all
the changes. It also contains new version of Atari XE/XL player of RMT
module files RMT1PLAY 1.01 - rmt1play.xex (4kb) and RMT versions of
well-known songs:"Hymn to aurora" [4:13] and "Turrican 2 noise 3" [5:24]
(revision 2).

And there is some extra bonus - new Atari XE/XL music demo rmtdemo.xex
(17kb). Enjoy it! :-)

http://www.infos.cz/raster/atari/rmt/rmt.htm

                            =~=~=~=

                        PEOPLE ARE TALKING
                       compiled by Joe Mirando
                         joe@atarinews.org

[Editor's note: Joe's column this week has been cancelled due to excessive
hexes, black cats, and ghosts from Atari HQ. A temporary detour roaming the
streets screaming "trick or treat" was also a factor!]

                            =~=~=~=

                     A-ONE's Headline News
               The Latest in Computer Technology News
                   Compiled by: Dana P. Jacobson

                Microsoft Unwraps New Operating System

Microsoft Corp. on Monday gave its most detailed look yet at the next
version of Windows, code-named "Longhorn," which promises new methods of
storing files, tighter links to the Internet, greater security, and fewer
annoying reboots.

At a conference for Microsoft programmers, Microsoft founder and Chairman
Bill Gates said Longhorn, when it arrives, would rank as Microsoft's
largest software launch this decade and the biggest since its Windows 95
operating system.

Gates and other Microsoft executives did not say when Longhorn would be
released, but promised outside programmers that the platform would
represent a breakthrough in the way that computer users send, receive and
work with information.

Applications built by outside developers for Windows have long been crucial

to the success of Microsoft's flagship software, which runs on more than 95 percent of the world's personal computers.

Jim Allchin, the Microsoft executive charged with the development of Windows, drew a lengthy round of applause when he announced one his main goals for Longhorn, ridding a scourge that has perpetually plagued Windows users.

"I'm on a campaign to get rid of reboots, not only in our code but in any of the code," he said.

Gates gave an upbeat and forward-looking address on the future of software, saying that much more needed to be done before it would allow users to realize the potential of inter-connected services.

"A lot of people nowadays are sort of pessimistic about what technology will bring," he told a packed audience at the Los Angeles Convention Center. "Certainly there is a lot of things Microsoft has to do."

For the next generation of software, Gates promised software advances like speech recognition and synthesis, integrated telephone services and better graphics.

"It's very clear we're at the beginning of this process," Gates told the developers. "We need your feedback. We need your involvement to get this right."

Microsoft said that Longhorn would tackle key problems facing computer users today - an overload of information and hard-to-find files.

"We see oceans of information," said Adam Sohn, a product manager for Microsoft's platform strategy and partner group, ahead of the presentation.

"There are a bunch of things going on that we find very interesting, and they're not necessarily all brand new, but they're gaining a lot of prevalence," he said.

During Gates' address, a Microsoft staffer gave a demonstration of Longhorn, highlighting among other features the "sidebar," an area on the right side of the screen capable of displaying messaging lists, stock quotes, news feeds, clocks, and pictures.

Sohn said Microsoft would not focus on the timing of the consumer release, although final versions of software usually follow the beta version by three months to a year.

The company also talked about the four key "buckets" it sees comprising Longhorn: fundamentals like security and scalability; new presentation technology that includes a rebuilding of Windows' graphics system; a new file storage system called WinFS that makes heavy use of XML, extensible markup language data; and new Web services and communications technology.

The company also unveiled "WinFX," which it described as a new application programming model for Windows that is the evolution of its .NET programming framework.

A demonstration of its next-generation storage technology, WinFS, featured a method to "stack" documents by author in a window, with the heights of the stacks corresponding to the number of documents, as well as file views that showed snapshots of documents, rather than just file names.

Allchin also showed "XAML," a declarative language for programming that would make it easier to create programs and features.

In the shorter term, Gates said Microsoft would have a beta version for the second service pack of its Windows XP operating system this year and a beta for the first service pack of the Windows Server 2003 system in the first half of 2004.

Apple Unleashes MAC OS Update 'Panther'

For the second time in just over a year, Apple Computer Inc. is out with a major upgrade of the Mac OS X operating system, packing it with features Windows users won't see for years and attaching a price tag befitting Apple's reputation as the Porsche of computer makers.

At $129 per computer or $199 for a five-license pack, Mac OS X 10.3 "Panther" is expensive, but for the most part worth the price. A variety of envelope-pushing enhancements improve navigation, security and interoperability with other computers.

The upgrade introduces an improved "Finder," the tool through which users poke around their hard drives and networks. It also solves the problem of desktop clutter, offers fast switching among users and provides strong security.

Most remarkably, despite the 150 improvements, Panther seemed to speed up, not slow, my aging Power Mac. After a tricky installation, the Unix-based operating system was rock solid and never crashed in my testing.

The most noticeable changes take advantage of the Mac's advanced graphics, which leap over the capabilities of Windows-based machines. Microsoft's next release, code-named Longhorn, won't introduce Windows users to similar features until 2006.

And these Apple graphics aren't just eye candy.

Panther exploits the advanced rendering capabilities to allow users to quickly make sense of a cluttered desktop. With the Expose (ex-poh-SAY) feature, all the open windows on the desktop immediately shrink to fit on the screen but are still clear enough to identify.

To bring a desired window to the foreground, the user need only to click on it. Another function key reveals all the windows in the current application. Yet another clears the desktop entirely. There was no stuttering or slow redrawing.

With Panther, Apple also introduces fast user-switching. Fans of Windows XP know this feature well: It allows one user to sign on while the previous user's programs continue to run in the background.

But Panther adds a graphical twist. When the account is switched, the entire screen becomes the face of a giant cube that appears to rotate, revealing another face of the cube with the new user's screen ready for action.

All applications continue to run for both users. In fact, while my wife

was checking e-mail under her username, my hidden session was still streaming iTunes music to my Windows network.

Apple also has made major strides in fixing the clunky Finder of previous releases. Besides a brushed-aluminum look, it sports a navigation pane that lists common areas such as the main hard drive, the applications folder and the network. Additional destinations can be added by dragging them into the pane.

Files that reside on the network are just as accessible as those on the local hard drives. In my mixed Mac-and-Windows network, all my PCs showed up after clicking the "network" icon and providing a username and password.

The networking improvements go a step farther. With printer-sharing enabled, any printer connected to the Mac can be shared with a networked PC. And a shared printer attached to a PC also can be shared with a Mac.

The benefits of such features are obvious in a corporate environment. Now, as home networking takes off, it's no longer necessary to run the same operating system on every computer.

With networking made simple, security becomes a greater concern.

Macs already have a reputation for being less prone to viruses than Windows computers. One reason is that Macs aren't as juicy targets as the legions of Windows machines. (Still, don't expect to escape the security patch: Apple released one for Mac OS X 10.3 on Tuesday.)

Another reason is that Apple tends to leave networking services off until the user decides to turn them on. Some versions of Windows are more vulnerable because Microsoft, before its recent security push, often left services on by default in the interests of user convenience.

Other security enhancements include an option to make files unrecoverable when they're deleted. Normally, on Windows machines and Macs, just the hard drive space is freed up when a file is removed. In Panther, users completely write over the freed-up hard drive space.

I experienced one rough spot with Panther - the installation. On my 2001 Power Mac G4, it could not boot from the installation CD.

Apple was as baffled as I, and according to the message boards at Apple's Web site, a handful of other users experienced the same problem. I eventually got the software installed by using the CD drive of a laptop I connected to the Power Mac via FireWire. Apple engineers are investigating the problem.

Once running, I had no other problems and could understand why Mac fans hold late-night launch parties even for an incremental upgrade. Panther doesn't disappoint.

Still, it would be nice if it weren't priced as if it were the Mac OS XI.

Internet Access Tax Ban Nears Vote

As the clock ticks toward Saturday's expiration of the federal ban on

Internet access taxes, lawmakers are angling to keep the moratorium, while cash-strapped states aim to make sure it doesn't cost them billions of tax dollars.

A bill making the moratorium permanent cleared the House in September and might make it to a Senate floor vote this week. A lingering key question: What constitutes Internet access, and what telecommunications services does such access include, if any. A number of senators have blocked action on the bill, HR 49, until the matter is clarified.

If passed, the bill would make permanent the current five-year moratorium on taxing Internet access. It would prohibit state and local jurisdictions from imposing new taxes on Internet access, either dial-up or broadband. The moratorium also would ban states from taxing online and offline purchases differently, such as imposing multiple taxes on an online purchase.

But the biggest sticking point is the definition of telecommunications services, which opponents call overly broad and ambiguous.

"Let's not be so vague. We could be permanently exempting telecommunications taxes that some states are now collecting," says Christine Lapille, a spokesperson for the National Governors' Association.

Others are concerned that services now taxed, such as phone service, could escape taxation in the future by being bundled with nontaxable Internet access.

The bill's language already makes clear that when a provider bundles taxable and nontaxable services, the entire package is taxable, says Mark Mullet, Verizon vice president of government relations.

"States and localities are blowing this up," Mullet says. "They're saying telephone companies are never paying another penny in tax again. That's just not true."

Nevertheless, according to the Multistate Tax Commission, states would lose between $4 billion and $9 billion in 2006 under the bill's provisions.

These numbers seem exaggerated, says Mike DiConti, director of the Business Roundtable, an industry group of the largest 150 American companies. Because technologies are so fluid today, lawmakers shouldn't be overly restrictive in their language, DiConti adds. "Not all contingencies can be written in today," he says. Sen. George Allen (R-Virginia), a cosponsor of the moratorium bill, is "working with senators on an individual basis on issues that they may have concerning the bill," according to Mike Waldron, an Allen spokesperson. Supporters say the bill has majority support in the Senate and should pass if it comes to a floor vote this week.

"This is not a partisan issue," says John Berthoud, president of the National Taxpayers Union. "If this comes to a vote, I think it's going to pass."

Sober-A Worm Pretends To Be Virus Fix

A new bilingual, mass-mailing worm is in the wild and plays off user fears about viruses.

Sober-A is spreading via e-mail on Windows systems; it arrives with German and English subject lines and an attachment that purports to be a fix for a bogus new worm. When executed, the worm searches the infected system for e-mail addresses to mail itself to using its own Simple Mail Transfer Protocol (SMTP) engine.

Helsinki, Finland-based F-Secure Corp. reported "a clear increase in reports of the Sober worm over the weekend," but most other antivirus companies have it listed as a low risk.

Some of Sober-A's subject lines and attachment names play off fears about viruses. Some of the subject lines include: "New internet virus!" "A worm is on your computer!" and "I love you (I'm not a virus!)," while some of the attachment names are Anti-Sob.bat, anti-trojan.exe, AntiVirusDoc.pif and security.pif.

Other subject lines are in German, a ploy that the writer apparently used in hopes of getting the worm to spread beyond the English-speaking world. This isn't the first time that a worm writer employed German and English phrases in a worm. Last May, the Fizzer worm traveled with subject lines and file names in German, Dutch and English.

Some of Sober's progress can be attributed to its use of more than one language. Mass-mailers, for the most part, rely on social engineering to trick unsuspecting computer users into opening the attached malware. "If you are in Korea or Vietnam and get a message in English, you probably won't even be able to read it, so you likely just delete it," said Chris Belthoff, senior security analyst at antivirus software vendor Sophos Inc.

Sober-A will be a minimal threat for enterprises, because most strip or block the file extensions that the worm employs. Generally, businesses have no need to allow e-mails containing executable files such as .pifs and .scrs. Those file types are used extensively by worm writers, and if such files need to be sent, there are other methods to transport them.

"At the end of the day, this is a mass-mailer," Belthoff said. "A user will need to double-click on the attachment to get it to execute."

Sober-A coincides with a comparative lull in malware activity. Observers are still waiting for worms to take advantage of new RPC-DCOM vulnerabilities in Windows announced last month. The flaws are very similar to the one that the Blaster worm exploited in August.

Also, experts are awaiting the next variant of the Sobig worm. The last one, Sobig-F, spread quickly in August, becoming one of the most virulent worms of all time. As with past variants, Sobig-F had an expiration date, so on Sept. 10 it stopped spreading. Experts think the family of worms are being used to create open relays for spammers, so it's just a matter of time before Sobig-G appears.

E-Mail Virus Turns PCs into Spam Machines

A new e-mail virus capable of turning infected personal computers into "spamming" machines emerged on Friday targeting corporate and home users in Europe and the United States, a computer security expert said.

Anti-virus software makers Trend Micro reported that tens of thousands of its corporate computer users in France and Germany were hit on Friday afternoon by the virus, dubbed "Mimail.C."

By 11:30 a.m. ET on Friday, there were reports of infections in the United States too, said Raimund Genes, European president of Trend Micro.

The firm had a "medium risk" rating on the bug. "We may be upgrading it to high risk if it spreads in the U.S.," he added.

The virus carries the subject message line "our private photos ???." Opening the e-mail triggers the virus into action.

The virus installs an SMTP, or simple mail transfer protocol, program on an infected PC that turns the computer into a type of e-mail computer server capable of sending out torrents of virus-infected messages, Genes said.

The e-mail has spread quickly because it spoofs e-mail addresses, making it appear as if the e-mail comes from a friend or co-worker. "It's an old spammers trick," said Genes.

The virus is not believed to be particularly damaging to the infected computer, but it has the potential to unleash a flood of virus e-mails that could bog down corporate networks, Genes said.

SCO Attacks Open Source License

Enlarging the scope of its lawsuit against IBM, SCO Group has filed court documents that challenge the validity of the GPL (GNU General Public License), the software license that governs Linux. If SCO were to successfully invalidate the GPL - which has never been legally challenged - it could have an enormous impact on Linux's future.

"The GPL violates the U.S. Constitution, together with copyright, antitrust and export control laws," states SCO in documents filed with the U.S. District Court for Utah.

"The GPL is effectively enforced by the Free Software Foundation such that the enforcement of the GPL by IBM or others is waived," claims SCO in court documents.

Eben Moglen, general counsel for the Free Software Foundation and Columbia University law professor, called SCO's claim "an act of self-parody."

"It's an indication of the desperation of SCO's legal position," he told NewsFactor. "By wrapping itself in big language about the Constitution and export control law, SCO is just trying to confuse people."

IBM attorneys are reviewing the documents that SCO submitted, IBM spokesperson Trink Guarino told NewsFactor "It appears that SCO has denied many of the facts supporting IBM's counterclaim. But IBM strongly believes its counterclaim and we look forward to trying this case in a court of law."

IBM's countersuit against SCO, filed in August, claims SCO violated the GPL, and in the process violated IBM's copyrights.

According to documents filed in court, IBM's countersuit seeks a ruling that "SCO is not entitled to impose restrictions on the copying, modifying or distributing of programs distributed by it under the GPL except as set out in the GPL."

IBM filed its countersuit in response to SCO's suit, filed in March, which alleges that IBM misappropriated source code from Unix - to which SCO owns the copyright - and incorporated it into Linux. IBM has denied this charge.

The GPL is the core set of rules by which Linux is developed and distributed. It allows any developer to modify a program's source code, under the condition that those modifications be made public when that program is distributed.

SCO currently distributes software under the GPL license, and also did so under its former name, Caldera International.

SCO's distribution of software under GPL contradicts its legal claims, Moglen said. "SCO has distributed under GPL for years, and continues to do so. That means that SCO has permitted everybody to copy, modify and distribute that code. They can't go back now and say people don't have a right to distribute that code.

"In order to run the scam that it is running, demanding people pay license fees to them for use of the Linux kernel, SCO has to say the GPL doesn't do what the GPL says it does," he argued.

If the GPL were invalidated, it could have a negative impact on many Linux vendors who work under the license agreement. It could create confusion regarding software copyright issues across the Linux industry, and also might undermine one of the key principles of open source: that software can be modified and shared freely.

But this outcome is unlikely, SuSE spokesperson Joe Eckert told NewsFactor. "Fortunately, we live in a country governed by the rule of law, and I think we'll find out that the GPL is pretty solid."

Printer Cartridge Clones Get Boost

A ruling this week from the U.S. Copyright Office could strengthen the defense in a copyright infringement lawsuit by Lexmark International that is expected to have broad effects on the market for low-cost, third-party printer cartridges.

Lexmark is suing manufacturer Static Control Components (SCC) of Sanford, North Carolina, which makes computer chips for third-party ink cartridges. The chips enable manufacturers to create clones of the cartridges used in Lexmark printers. Lexmark sued SCC last year, charging that SCC's chips contain copyrighted Lexmark computer code and consequently violate the Digital Millennium Copyright Act (news - web sites) (DMCA) ban on circumventing digital technology that protects copyrighted material.

Without taking a position on whether SCC's chips illegally incorporate Lexmark code, the Copyright Office has ruled that the DMCA does not block such usage. Software developers can use reverse engineering to circumvent digital protection of copyrighted material, if they do so to achieve interoperability with an independently created computer program.

The SCC had asked the Copyright Office to recommend several DMCA exemptions that would protect its efforts to defeat Lexmark's protection technology. The requested exemptions are unnecessary because existing DMCA statutes already permit the kind of reverse engineering that SCC could use to thwart Lexmark's protections, the agency said in a lengthy memo of recommendations about DMCA exemptions.

SCC executives hailed the Copyright Office's statement as a watershed moment for their case.

"We think the Copyright Office put to rest all of the objections Lexmark has raised," said SCC CEO Ed Swartz.

Lexmark responded that it was pleased the Copyright Office refused SCC's exemption request.

"It is inconceivable to us how anyone can consider this ruling a victory for Static Control," said Vincent Cole, Lexmark's general counsel, in a prepared statement. Lexmark refused further comment on the agency's memo.

SCC pulled its Smartek chips for Lexmark clone cartridges from the market earlier this year in accordance with a preliminary injunction favoring Lexmark. U.S. District Court Judge Karl Forester found that SCC directly copied Lexmark's copyrighted Toner Loading Program - a charge SCC admits is accurate - and ruled that its efforts to bypass Lexmark's authentication controls violated the DMCA.

The latter half of that ruling could be affected by the Copyright Office's recommendation. SCC was already pursuing an appeal of the injunction, and the company expects the appeal to be heard later this year.

The fight between Lexmark and SCC may have implications throughout the lucrative market for printer cartridges, according to some industry analysts. Printer manufactures earn substantial margins selling printers cartridges. Third-party manufacturers have carved out a chunk of that market by offering refurbished cartridges for a fraction of the cost of those from the printers' original makers.

Last year Lexmark began using a chip in some of its cartridges that communicates with the company's printers and verifies that the cartridge is from Lexmark. Without that verification, the cartridge won't work. SCC's Smartek chips mimic the Lexmark chips so third-party cartridges can pose as official ones.

SCC is confident that the Copyright Office memo green-lights its Smartek chips, Swartz said. Of the court's finding that SCC's chips illegally use Lexmark code, Swartz said that the Copyright Office ruling may excuse the code use - but if not, SCC will develop new code that meets the requirements of the reverse-engineering exemption.

A research report from Merrill Lynch suggests that Lexmark could thwart SCC by advancing its software so that reverse engineering would be technically infeasible, but Swartz brushed off such concerns.

SCC already offered to show Lexmark the software it has developed to replace the infringing code in its Smartek chips, Swartz said. Lexmark refused to authorize that approach, citing DMCA protections against any authentication bypass maneuver, according to Swartz.

"I think that what the Copyright Office saw here was that what was taking place was a test case," Swartz said. "If they came down on the side of Lexmark, what they would be doing would be to provide a path for companies to develop a legal electronic monopoly that would make the oil trust and the steel trust that Teddy Roosevelt broke up at the turn of the century look small."

CAN-SPAM Law Won't, Critics Say

The first federal antispam law may be on its way to reality, but many antispam advocates say it won't stem the flood into e-mail users' in-boxes.

The Senate unanimously approved the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act last week. It requires e-mail users to opt out of unwanted commercial e-mail, instead of requiring e-mail senders to get permission before sending. That approach is backwards, say vendors of antispam technologies and at least one consumer advocacy group.

The bill gives consumers little control over spam, says Ray Everett-Church, counsel for the Coalition Against Unsolicited Commercial Email (CAUCE). Everett-Church says he is encouraged that the bill includes an amendment requiring the Federal Trade Commission to consider a national do-not-spam e-mail registry, but it doesn't require the FTC to actually implement such a list.

A 1991 law authorized the Federal Communications Commission to create a national do-not-call telemarketing registry, which took effect in early October - 12 years later, Everett-Church notes. The FTC has expressed concerns about creating and maintaining a massive do-not-spam list, and CAN-SPAM's opt-out approach basically lets spammers continue to e-mail until they're told to stop, he adds.

"Until the FTC decides whether or not they care to create a do-not-e-mail list, [CAN-SPAM] creates essentially carte blanche permission for spammers to send unlimited quantities of e-mail to the consumer," Everett-Church says. "I'm deeply concerned that we may never see a do-not-e-mail list, and until such a time as we do, we will see an unlimited right to see spam."

The CAN-SPAM Act requires commercial e-mail senders to provide valid opt-out mechanisms. It fines senders up to $100 per e-mail message sent with misleading header information, and supports fines of up to $3 million for some types of spam. But Everett-Church questions whether state and federal law enforcement agencies have the time to go after spammers, especially since CAN-SPAM does not provide additional funding. The FTC and state attorneys general are responsible for most spam enforcement under the bill.

Cosponsors of the bill, Senators Conrad Burns (R-Montana) and Ron Wyden (D-Oregon), defend it, saying it is one necessary piece in a multipronged fight. Technology also needs to be part of the spam wars, but CAN-SPAM should send a "strong message" to spammers, said a Burns spokesperson.

"No legislation will be a silver bullet against spam, but the Burns-Wyden legislation gives consumers considerable control over the e-mail coming to their in-boxes by backing up the law's requirements with stiff civil and criminal penalties," says a Wyden spokesperson, responding by e-mail. "This

is a good step toward taking back the Internet from the 'kingpin spammers' - the worst actors of the online world."

Not surprisingly, vendors of antispam technologies agree technology should part of the solution. Some suggest antispam technologies will go further to help e-mail users than CAN-SPAM will. The spirit of the law is headed in the right direction, and CAN-SPAM can help set a moral tone against spam, says Dave Jevans, senior vice president of marketing at Tumbleweed Communications, an e-mail firewall vendor.

He says CAN-SPAM isn't even enforceable. It's difficult to validate the identity of any Internet user, and a large percentage of spam comes from outside the U.S., he notes. CAN-SPAM might make some potential spammers think twice before getting into the business, but spam continues to double about every two months, he says.

"The growth will outweigh by far the amount of spam stopped by CAN-SPAM," Jevans says. He urges a blend of legislative and technological approaches. For example, e-mail could be required to carry a digital signature establishing the sender's identity, he says.

Another antispam vendor is even more pessimistic about CAN-SPAM's effectiveness. A law might stop legitimate marketers from using spam techniques, but it does nothing to stop hackers from using spam as a tool for identity theft, says Pete Privateer, senior vice president for product strategy and marketing at security and antispam vendor Internet Security Systems.

"This bill is like trying to write a law to ban viruses," Privateer says. "It's just about that effective. I expect the volume of traffic in your in-box to increase."

But Al DiGuido, chief executive officer of e-mail marketing services provider Bigfoot Interactive, says CAN-SPAM will at least clear up the confusion of more than 30 state laws dealing with spam. "We're really excited about federal guidelines that will put an end to all the chaos and confusion on a state-by-state basis," he says.

DiGuido agrees with Wyden that legislation should be only one part of the strategy in the spam wars. He recommends reputable marketers work on a fee-based e-mail system, where they pay a small fee to ISPs to create whitelists, which list commercial entities that are permitted to send e-mail, to ensure that their messages are delivered.

"There will be some real teeth put behind the law that will impose jail terms and significant penalties from a dollars and cents standpoint," DiGuido says. "We also think...the criminal element has been trying to evade the law for some time now, so they'll continue to try to find ways to evade the law."

                    House Could Vote Soon on Senate Anti-Spam Bill

The U.S. House of Representatives could vote as early as next week on a bill to outlaw e-mail "spam" that has already passed the Senate, congressional aides said on Thursday.

House leaders could take up the Senate bill to avoid choosing between two

competing House bills that have effectively checkmated each other at the committee level, the aides said.

As the volume of get-rich-quick schemes, body-enhancement offers and other unwanted spam has grown to account for more than half of all e-mail traffic, pressure has increased on Congress to outlaw much of the unsolicited commercial e-mail.

The Senate passed an anti-spam measure by a vote of 97-0 last week, but similar legislation in the House has been stalled at the committee level.

Leaders of the House Energy and Commerce and Judiciary committees introduced an anti-spam bill earlier this year, but many rank-and-file members support a tougher bill introduced by New Mexico Republican Rep. Heather Wilson.

The two sides have made no progress since July and passage of either House bill is seen as unlikely this year.

Energy and Commerce Committee Chairman Billy Tauzin could bypass the logjam by taking up the Senate bill and bring it directly to the House floor without a committee vote, several aides said.

"It's an option that's being discussed, but no final decisions have been made," Tauzin spokesman Ken Johnson said.

A spokesman for House Speaker Dennis Hastert similarly said that House leaders are considering the approach but have not yet made any decisions.

Both House bills show many similarities to the Senate's Can Spam Act, which was sponsored by Montana Republican Sen. Conrad Burns and Oregon Democratic Sen. Ron Wyden.

Businesses would be free to send unsolicited e-mail to Internet users, but would have to identify themselves clearly and honor requests to be taken off their mailing lists. Violators would face fines and jail time.

But the bill could face opposition from dozens of supporters of Wilson's bill, who favor a broader definition of spam and more latitude for state prosecutors to pursue spammers.

"She still has concerns about enforcement and the definition of commercial e-mail that is contained in the Can Spam Act, and so at this point she thinks those are things that we have to continue to address," a Wilson spokesman said.

UK Lawmakers: We Will Extradite Overseas Spammers

British lawmakers plan to use a new tactic to stop the torrent of junk e-mail spam that floods in from overseas: extradite the mass-mailers and bring them to trial in the United Kingdom.

"Spammers are no longer an irritant, they are a threat," British MP Brian White told Reuters on Thursday. The UK last month was the second European Union (news - web sites) country after Italy to criminalize spam in a law that goes into effect in December.

But the law has drawn criticism from anti-spam crusaders who say it will be powerless to stop the flood of messages at the source. The majority of spam originates overseas, and in particular, the United States, industry experts say.

While initially, extradition would be used to target spammers, it could be expanded to include suspects in other cybercrime cases such as virus-writing and hacking, he added.

White said he and fellow British lawmakers traveled to the U.S. earlier this month where they discussed with FBI officials extraditing American spammers who violate British laws.

"The FBI's reaction was, subject to the individual case, they couldn't see any problem with it," he said.

UK and U.S. law enforcement authorities have a long history of cooperation in criminal matters, a relationship that has only grown stronger in the wake of the September 11, 2001 attacks in America and their subsequent crackdowns on subversive groups.

The rise of spam, that flood of unsolicited e-mail offering everything from pornography and cheap mortgages to a full head of hair, has become an urgent matter for lawmakers around the world.

Lately, law enforcement officials have begun to crack down on spam as a growing amount contains child pornography and spam messages have been used in a spate of recent fraud scams that target online banking customers.

White said spammers could be extradited if they violated the Computer Misuse Act, a 13-year-old UK law that makes it illegal to tamper with and damage another user's computer.

Therefore, a spammer who sends e-mails that contain viruses or so-called trojans, programs capable of taking over another user's computer, would be grounds for extradition, White said.

"The majority of spam is either breaking the law regarding fraud, obscenity, child pornography, or (distribution and marketing) of prescription drugs. We wouldn't get every spammer under all three of those laws, but you could get a majority," he added.

The challenge for prosecutors will be building up a strong enough case linking spammers with a particular crime as most operate under aliases and have effectively disguised their whereabouts.

White said the All Party Internet Group, a collection of parliamentarians who have been pushing Internet-related legislation, has asked for the UK's Home Office to update the Computer Misuse Act of 1990, a law written before the advent of the World Wide Web.

The current law, he said, is not equipped to deal with the modern day nuances of cybercrime.

Anti-Spam Law Goes Into Force in Europe

European Union digital privacy rules came into force Friday requiring

companies to get consent before sending e-mail, tracking personal data on Web sites or pinpointing callers' locations via satellite-linked mobile phones.

The law steps up the global war on spam and "is a key tool to strengthen consumer confidence in the Internet and electronic communications," said EU Enterprise Commissioner Erkki Liikanen.

But how the enforce the new rules are left to the 15 EU nations. Fines vary among the countries, and unlike the strictest laws in Virginia and other U.S. states, European Union rules don't call for jail time.

And although the EU rules cover spam sent from the United States and elsewhere, member countries lack both the resources and the authority to pursue violators abroad.

Most spam comes from the United States, where the Senate recently approved a do-not-spam list and a ban on sending unsolicited commercial e-mail using a false return address or misleading subject line. Several states also have anti-spam laws.

Nonetheless, Europe has been more aggressive at adopting measures protecting peoples' right to be left alone.

The new European rules also limit companies' ability to use "cookie" files and other devices that let them obtain information about users who visit their Web sites. Companies will now be required to ask users' permission before taking such data and retaining or selling it.

"Spyware" that burrows invisibly onto computer hard drives and snoops on users also becomes illegal.

Europe will allow only police and emergency services to locate people from their satellite-linked mobile phones.

"The directive is technology neutral and gives consumer and citizens a variety of tools to protect their privacy and personal data," the European Commission said in a statement.

Microsoft Settles Six Class Action Suits

Microsoft has settled antitrust class action lawsuits with five states and the District of Columbia, the company announced Tuesday.

The six new settlements, with a total value of about $200 million, brings the total number of states that have settled to 10. Class action lawsuits against Microsoft for antitrust-related practices continue in five states.

The total cost to Microsoft of all 10 class-action lawsuits it has settled is about $1.55 billion, including a $1.1 billion settlement of a California lawsuit in January.

Two of the six settlements discussed Tuesday, with Kansas and the District of Columbia, have been granted preliminary approval by the overseeing courts, said Brad Smith, Microsoft senior vice president and general counsel. The settlements, in the form of hardware or software vouchers to past purchasers of Microsoft software, will be $32 million for Kansas and

$6.2 million for the District of Columbia.

Settlements in four other states - North Carolina, Tennessee, North Dakota, and South Dakota - have not been approved by courts, and Microsoft did not release the details of those settlements Tuesday.

The six new settlements are similar to settlements Microsoft has announced with Montana, California, Florida, and West Virginia. Half of the value of any unclaimed vouchers will go to needy schools in the settling states. The schools can purchase hardware, software, or technical training with the money, and neither the consumers nor the schools are required to purchase Microsoft products with the vouchers.

Class-action lawsuits remain in Arizona, Iowa, Minnesota, New Mexico, and Wisconsin.

Microsoft Goes After Google

Microsoft has reportedly approached Google about a potential buyout of the search technology company.

Mountain View, California-based Google, one of Silicon Valley's few business success stories in the post-dot-com era, has been meeting with investment bankers over the last several months and exploring its options for a public offering.

During that process, Microsoft approached Google to discuss alliance options, including a takeover, according to an article in Friday's New York Times.

Google hasn't been rushing to take Microsoft up on the offer: Executives there seem to favor a public offering rather than an acquisition, the newspaper reported.

Microsoft and Google declined to provide comment to the New York Times for its story.

Calls placed to both companies by IDG News Service weren't immediately returned.

Microsoft has been looking into the Web search market now largely dominated by five-year-old Google.

While Microsoft has denied plans to enter the paid search industry, it has increased the staff on its search team to more than 200 and deemed MSN Search one of the company's key businesses.

Students Develop File-Swap Alternative

Keith Winstein and Josh Mandel may soon be the most popular guys on campus. They say they've discovered a way to give their fellow students at MIT and elsewhere dorm-room access to a huge music library without having to worry about getting slapped with a lawsuit from the recording industry.

On Monday, the pair planned to debut a system they've built that lets MIT students listen for free to 3,500 CDs over the school's cable television network. They say it's completely kosher under copyright law.

The students will share the software with other schools, who they say could operate their own networks for just a few thousand dollars per year. They call that a small price to pay for heading off lawsuits like those the recording industry filed against hundreds of alleged illegal file-swappers.

Here's the catch: The system is operated over the Internet but the music is pumped through MIT's cable television network. That makes it an analog transmission, as opposed to a digital one, in which a file is reproduced exactly.

The downside is the sound quality: better than FM radio, but not as good as a CD.

But the upside is that because the copy isn't exact, the licensing hurdles are lower. The idea piggybacks on two things: the broad, cheap licenses given to many universities to "perform" analog music, and the same rules that require radio stations to pay songwriters, but not record companies, to broadcast songs.

It also can broadcast any CD - even ones by popular artists like Madonna and the Beatles who have resisted making their songs available even to legal digital download services.

"I think it's fascinating. As a copyright lawyer, I think they've managed to thread the needle," said Fred Von Lohmann, a lawyer for the San Francisco-based Electronic Frontier Foundation. "They've basically managed to cut the record labels out of the equation altogether."

Conceivably, the system could be replicated by the cable system of a city or town, the students said.

But it seems ideally suited for universities, which often operate internal cable networks, and already have these broad performance licenses. College students are among the most enthusiastic file-swappers, and universities are exploring ways, such as fee-based systems, to give their students legal access to music.

The MIT project is called "Library Access to Music," or "LAMP," and here's how it works: Users go to a Web page and "check out" one of 16 cable channels in the MIT system, which they can control for up to 80 minutes. The controller then picks songs from among 3,500 CDs - all suggested by students in an online survey over the past year - that Winstein, 22, and Mandel, 20, have compiled.

The music is then pumped into the user's room on that channel and played through a TV, a laptop with an audio jack or external speakers.

Only one person controls each channel at a time, but anyone can listen in. Anyone can also see on another channel what selections are playing and the usernames of the controllers (Winstein acknowledges potential privacy concerns, but there are upsides: He once got a romantic proposition from a user who admired his taste for Stravinsky).

If all 16 channels regularly fill up, MIT could make more available for a few hundred dollars each. Users can listen to, but not store, the music.

The students built the system using part of $25 million grant to MIT from Microsoft Corp., some of which was set aside for student projects.

"We still wanted to do it over the Internet, but MIT's lawyers were not willing to chance that," Winstein said.

Their solution required navigating an alphabet soup of licensing groups. A big challenge was confronting two sets of copyrights: those held by the songwriters on the songs, and those held by record labels on the recordings of the songs. Under the latter, it wasn't clear MIT could simply make available the thousands of CDs MIT already owns in its library.

Instead, the students waited for the National Music Publishers Association's licensing arm to authorize a Seattle company called Loudeye to sell the students MP3s of the 3,500 CDs their fellow students had suggested. The students then paid Loudeye $8 per CD for the MP3s (they plan to expand the collection as students request more music).

A spokesman for the Recording Industry Association of America, Jonathan Lamy, was provided with a description of the project and, after consulting with RIAA colleagues, declined comment on it.

The students say that because they've done the licensing legwork, other schools could easily follow. All it would take is about $40,000 to cover hardware and a CD collection.

Von Lohmann said that if record labels would grant blanket licenses, as songwriters have, systems like MIT's could handle digital music and solve the peer-to-peer controversy.

"The students get access to a broad array of music, and the copyright owners get paid. This is where we should all be heading," Von Lohmann said. "I hope the record industry takes note and realizes this is a whole lot more promising than suing people."

E-Mails, Digital Media Produce Data Mountain

All those e-mails - junk or otherwise - are adding up.

In 2002, people around the globe created enough new information to fill 500,000 U.S. Libraries of Congress, according to a study by faculty and students at the University of California at Berkeley.

The 5 billion gigabytes of new data works out to about 800 megabytes per person - the equivalent of a stack of books 30 feet high - the study by the university's School of Information Management and Systems found.

That's a 30 percent increase in stored information from 1999, the last time the global study was conducted.

The information area with the biggest percentage increase in data was, unsurprisingly, hard disk drives. The study found the amount of stored information on these increasingly high-capacity storage media rose by up to 114 percent from the previous study in 1999.

The study also put to rest any lingering myths about the paperless office. The amount of information stored on paper, including books, journals and

office documents, increased up to 43 percent in 2002 compared to 1999.

"We thought in our (last) study that film and paper would head toward digital formats," UC Berkeley Professor Peter Lyman said.

With paper, that has not been the case, as people access documents on their computer, but then print them out, he said.

But photography is fulfilling his initial expectations.

"Individual photographs are really moving quickly to digital cameras, or even image-producing telephones," Lyman said. That helped contribute to a decline of up to 9 percent in film-based photographs in 2002 compared with 1999, and fueled the growth of magnetic storage.

The study received financing from Intel Corp., Microsoft Corp., Hewlett-Packard Co. and EMC Corp., technology companies whose businesses deal with managing information.

In addition to looking at stored data, UC Berkeley measured electronic flows of new information at 18 billion gigabytes in 2002, of which about 17.3 billion gigabytes occurred over the telephone.

Whether or not that information has any value is another question.

"I couldn't come up with a very simple way of understanding quality because it's so much in the eye of the beholder," Lyman said.

How, or if, all that information actually ends up being used will be the topic of his next study, Lyman added.

The Ten Commandments of PC Security

And it was written (by Bill Gates, et al): Thou shalt use a Windows PC to do thy work and it will be good.

But Windows computers are vulnerable to plagues of biblical proportions: viruses that bring down entire networks, e-mail worms that replicate at lightning speed, Trojan horses that hide inside otherwise innocent programs, hackers that take over computers, and more.

Fortunately, archeologists have recently unearthed two stone tablets from a garage near Cupertino, California that can help deliver us from such evils. We present their guidelines here, along with interpretations from our brothers and sisters in the PC security choir.

I. Remember thy antivirus software and keep it updated. It's not enough to have the software installed (if you don't have an antivirus package, stop reading right now and get one); you also need to keep up with new viruses as they emerge. "Your antivirus software is only as good as your latest virus definitions set," says Kelly Martin, senior product manager for Symantec's Norton AntiVirus. Programs like Symantec's Norton AntiVirus ($50) and Network Associates' McAfee VirusScan ($35 to $60) can automatically update their virus signature databases, but it costs an additional $20 to $35 for ongoing annual subscriptions.

II. Thou shalt not covet thy neighbor's attachments. You get a message you

think is from a friend with what looks like a cool file attached, so you click on it. Next thing you know, you're Typhoid Mary, spewing out infected e-mails to everyone in your address book. That's how the Sobig.F worm spread - and it happened so quickly that millions of copies got out before the antivirus companies could update their databases.

"Never trust an e-mail 'from' address," adds Chris Wysopal, director of research for security consultants @Stake. "And never open an attachment without verifying it was sent by a trusted person, and they meant to send it to you."

III. Avoideth bogus file downloads. Be wary of any Web site that requires you to download software to view a page, unless it's something familiar like a Flash plug-in or Acrobat Reader. The file may contain a virus, a Trojan horse, or some auto-dialer that calls pay-per-minute numbers via your modem and racks up huge charges.

"Do not install software via the Web unless you are absolutely sure what it is and that you trust the company you are downloading it from," warns @Stake's Wysopal.

IV. Smite spyware and pop-ups. Like Trojan horse programs, spyware secretly installs itself when you download software like file-swapping applications; it tracks your movements online and delivers ads based on where you surf. Pop-up ads can also exploit security flaws in Internet Explorer, like the recent Qhost Trojan that hijacked users' browsers after they viewed an ad on the Fortune City Web site. Fortunately, there are tools that can protect you: For example, Ad-aware (free) blocks spyware and StopZilla ($30) takes care of pop-up ads. Some antivirus software and security suites also stop spyware and pop-ups in their tracks.

V. Thou shalt foil spammers. Unsolicited commercial e-mail is more than just a nuisance; it's also a major source of virus infections. In fact, some versions of Sobig are designed to turn infected PCs into zombie machines that can be used to send spam. A good filter like Symantec's Norton AntiSpam 2004 ($40), Network Associates' McAfee SpamKiller 5 ($40 to $50), or Sunbelt Software's IHateSpam ($20) help trap the nasties your antivirus software might miss.

VI. Keep thy operating system patched. E-mail-borne worms and other scourges like to exploit security holes in your software - namely Windows and other Microsoft programs. These days Microsoft issues so many critical updates to fix these flaws that many users ignore them. Don't. Last January, the Slammer worm exploited a vulnerability that Microsoft had fixed more than six months before. But thousands of infected computers - including some at Microsoft - didn't have the patch installed. Run the Windows Update program once a week and whenever Microsoft issues a warning.

"Until we see automated patch management software, users will simply have to stay up to date," says Thor Larholm, senior security researcher at PivX Solutions.

VII. Maketh a rescue disk and keep it handy. When things go bad, a boot or rescue disk is your first step to recovery. At minimum, you'll want to put the basic elements of your operating system on a floppy disk or Zip media, so you can bypass the hard disk at start-up. To find out how, read "Hardware Tips: Create Your Own Emergency Boot Disk." A better idea: Use your antivirus program to create a rescue disk you can use when your system gets infected. Label it with a date and store it near your system where you won't lose it.

VIII. Be not taken in by false claims. There are more hoaxers than hackers
on the Internet, and more bogus "e-mail virus alerts" than actual viruses.
Even real virus threats are typically blown out of proportion by the media.
A phony warning could cause you to delete harmless files and then forward
the message to others, clogging e-mail servers and causing virus-like
damage in the process. When you get one of these e-mails (or see yet
another breathless news story), check it out first. Type the name of the
alleged virus into a search engine to see if any of the major security
vendors have issued an alert, and visit the virus hoax pages at F-Secure
and Hoaxbusters.

IX. Honor thy firewall. A firewall is like a bouncer for your computer - it
checks every ID at the door and won't let anything in or out until you give
the thumbs up. So a hacker can't access personal information on your hard
drive, and a Trojan horse keystroke logger (a stealth program that monitors
the characters you type) can't steal your passwords and transmit them over
the Net. Symantec and Network Associates both offer personal firewall
packages for $35 to $50, while Zone Labs offers a no-frills version of its
ZoneAlarm software firewall for free. But a better deal is an Internet
security suite that combines antivirus, firewall, ad blockers, spam
fighting, and other useful apps; most cost between $60 to $80. For a review
of suites from Symantec and Network Associates, read "Extra-Suite Virus and
Spam Protection."

X. Maketh backups and keep them holy. Simply put: Back up your data files
at least weekly (daily if you're running a business). Even if you fall
victim to a virus or hacker attack, you'll escape with only minor damage.
Fail to keep a recent backup though, and you'll go straight to hell - at
least, that's how it will feel.

                                  =~=~=~=